ICTACADEMY®

TATA STRIVE | Right Skills Bright Future

Need for Cyber Security

Ecosystem of Cyber Security

Feb 2021

TATA TRUSTS

Agenda

In today’s session, you will learn about:

- Cyber Security Framework
- The Framework Core
- Attack Matrix

Source: Freepik

Cyber Security Framework History

February 2013

Executive Order 13636: ***Improving Critical Infrastructure Cybersecurity***

December 2014

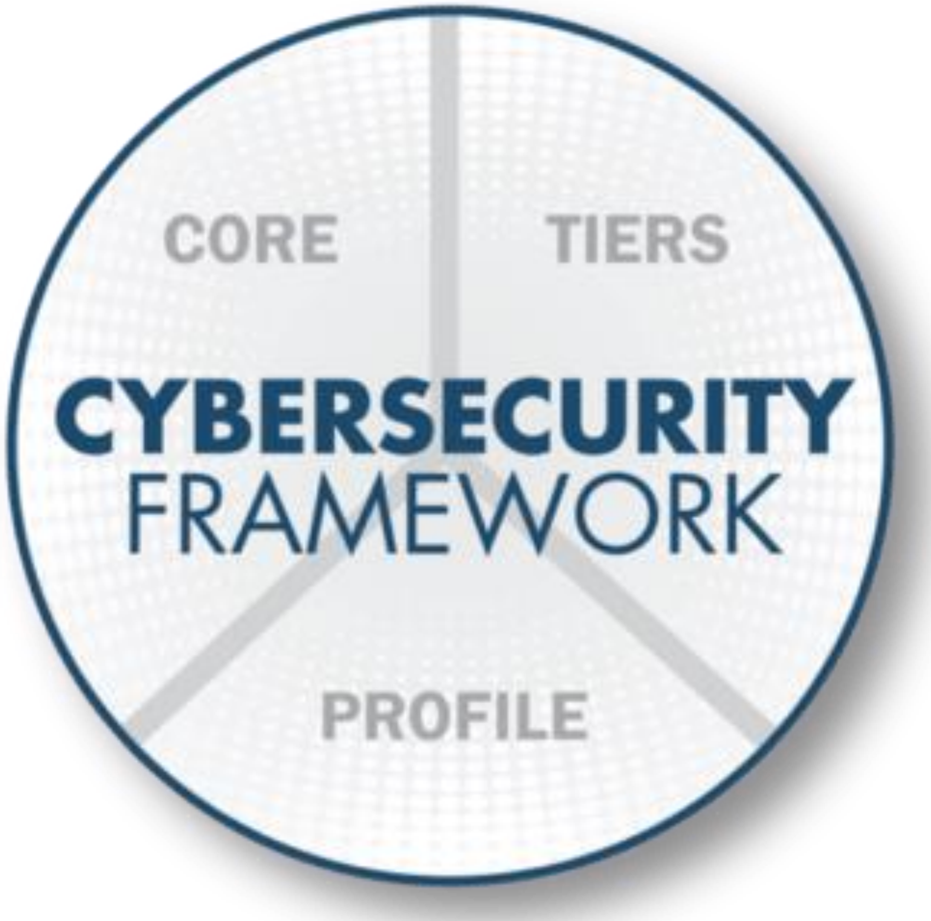
Cybersecurity Enhancement Act of 2014

May 2017

Strengthening the ***Cybersecurity of Federal Networks and Critical Infrastructure***

The Cyber Security Framework

The three Primary Components of Cyber Security Framework



Activity

Name of the Activity

Identify the Component

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Identify the Components

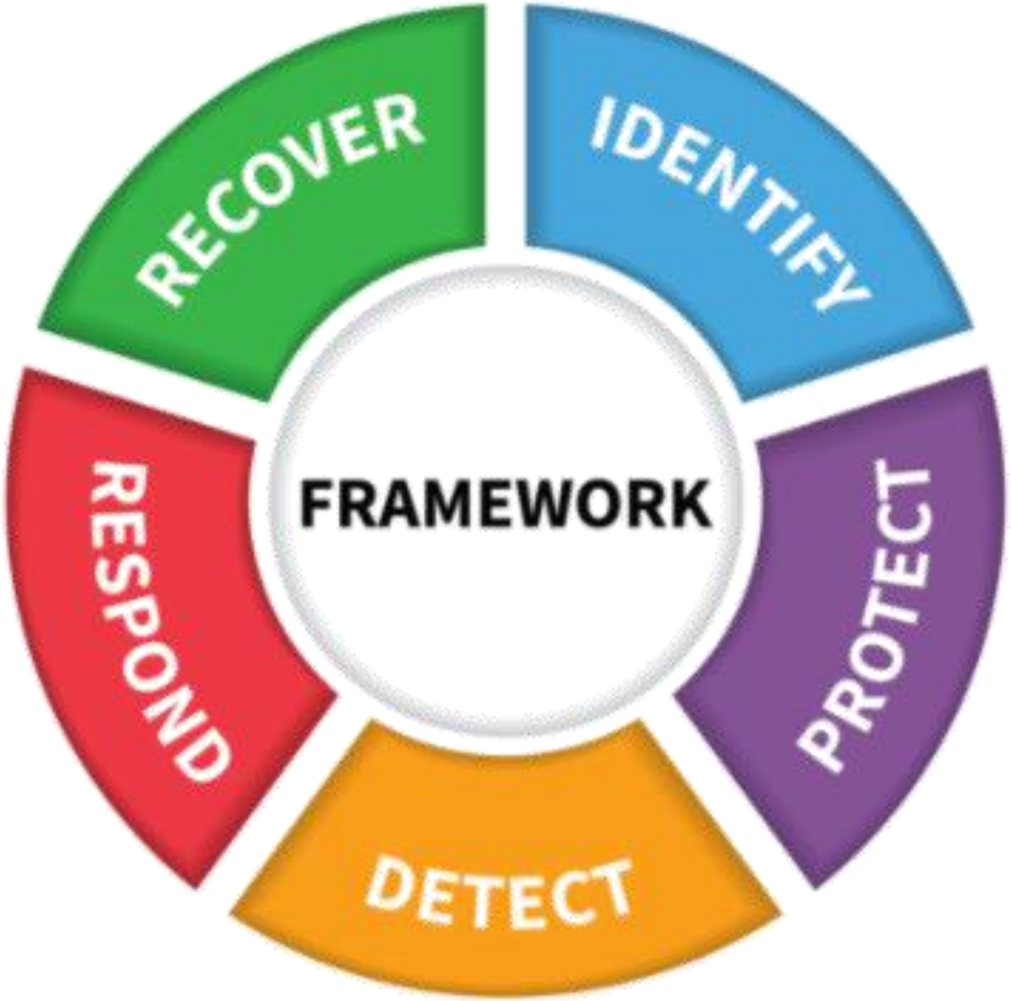
- This component is the desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls. **Core**

- This component is a qualitative measure of organizational cybersecurity risk management practices. **Implementation Tiers**

- This component aligns an organization's requirements and objectives, risk appetite and resources using the desired outcomes of the Framework. **Profile**

Key Framework Attributes

The Framework Core consists of five attributes



Activity

Name of the Activity

Who am I?

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Who am I?

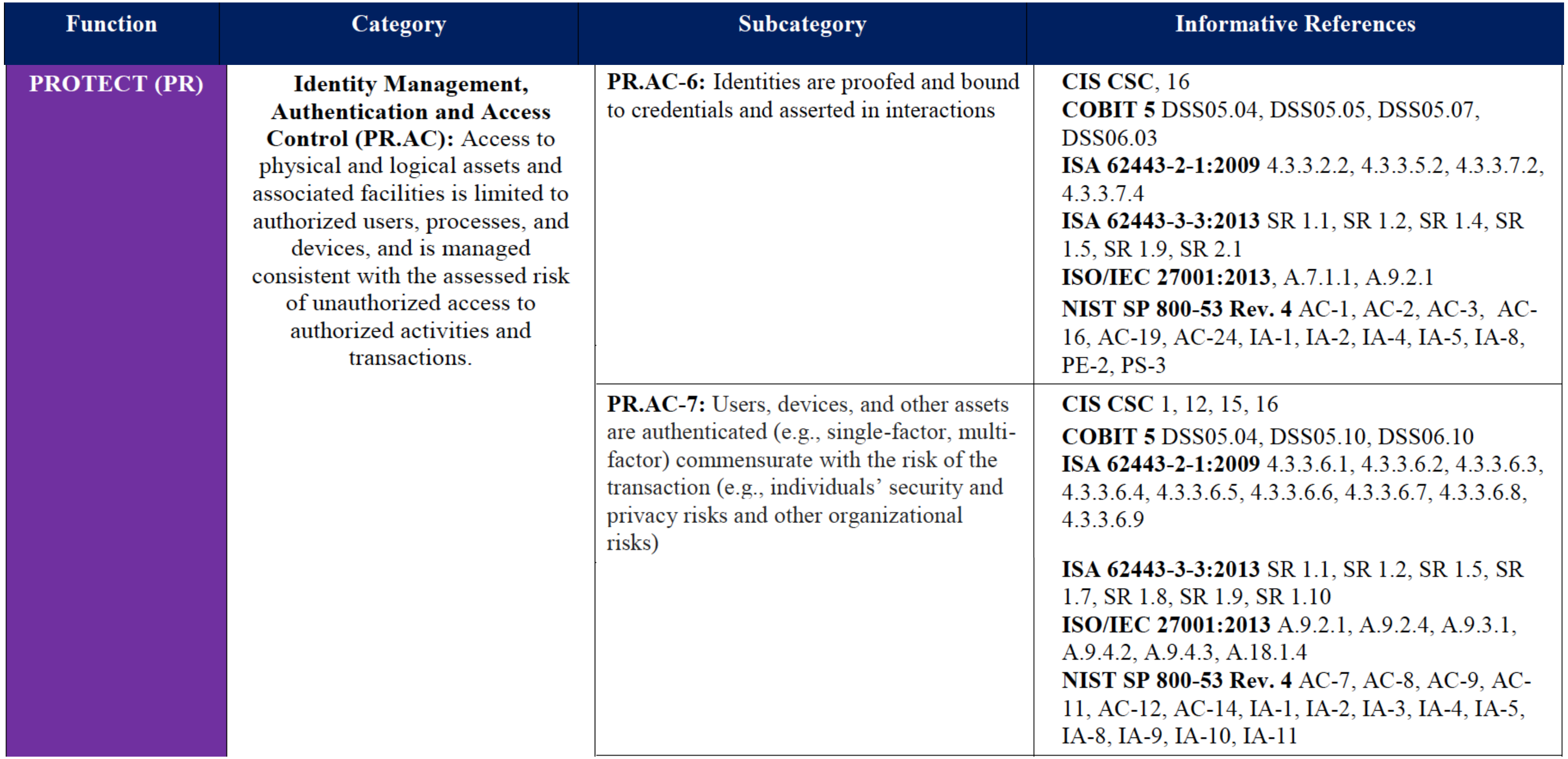
- I am responsible for developing the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. **Identify**
- My activities enable timely discovery of cybersecurity events **Detect**
- I am responsible for developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services. **Protect**
- My role is to develop and implement the appropriate activities to take action regarding a detected cybersecurity event. **Respond**

The Framework Core - Benefits

Function
Identify
Protect
Detect
Respond
Recover

- Describes desired outcomes
- Understandable by everyone.
- Applies to any type of risk management.
- Defines the entire breadth of cybersecurity.
- Spans across both prevention and reaction.

An Excerpt from the Framework Core



Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

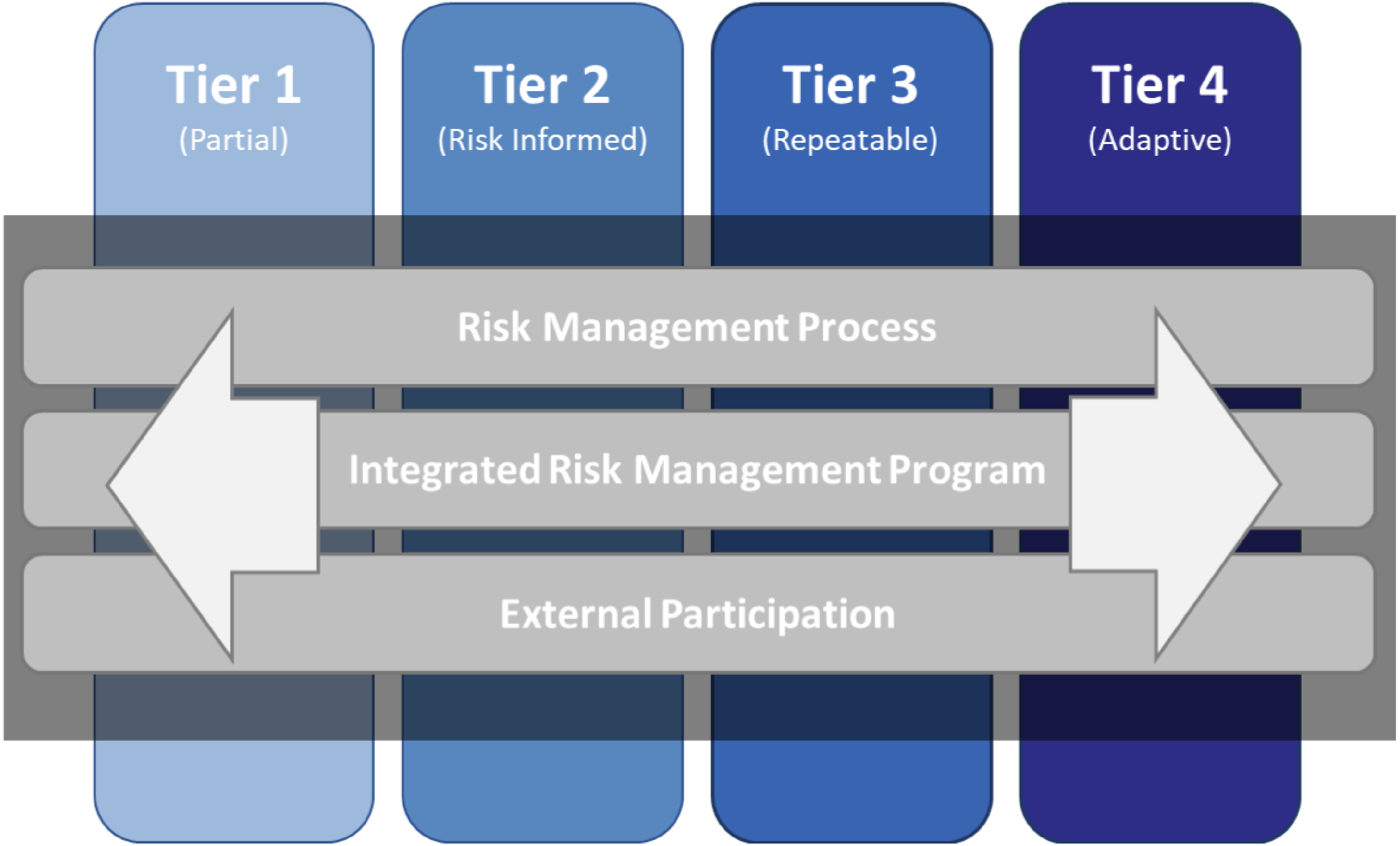
5 Functions

23 Categories

108 Subcategories

6 Informative References

Implementation Tiers



Source: NIST

Activity

Name of the Activity

Complete the image

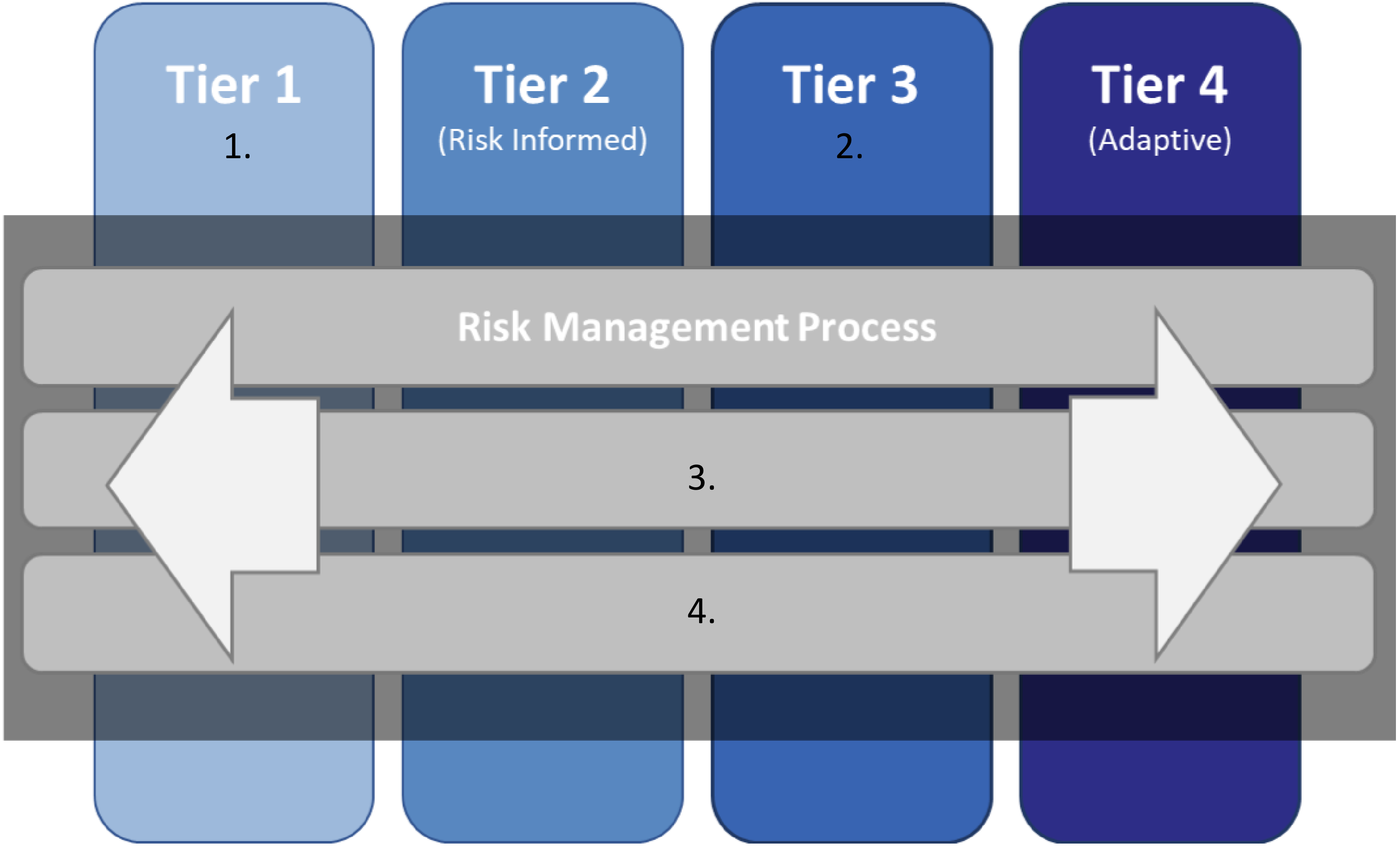
Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Complete the Image



Tier 1
1.

Tier 2
(Risk Informed)

Tier 3
2.

Tier 4
(Adaptive)

Risk Management Process

3.

4.

Think-Tank

What is the Attack Matrix?

Created by fae frey
from Noun Project

ATT&CK Framework

- MITRE developed **ATT&CK** as a model to document and track various techniques attackers use throughout the different stages of a cyberattack to infiltrate your network and exfiltrate data.

- ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge.

ATT&CK and Cyber Kill Chain

ATT&CK

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration
- Command and Control

Cyber Kill Chain

- Reconnaissance
- Intrusion
- Exploitation
- Privilege Escalation
- Lateral Movement
- Anti-forensics
- Denial of Service
- Exfiltration

Activity

Name of the Activity

Face Off

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Face Off

ATT&CK

v/s

Cyber Kill Chain

MITRE ATT&CK Matrices

- There are several different matrices:

PRE-ATT&CK

Windows

Linux

MacOS

Mobile ATT&CK

Tactics and Techniques

Red Team

Pentesting Attackers

Uses ATT&CK to develop a plan using multiple techniques to test the strength of their target.

Blue Team

Pentesting Defenders

Uses ATT&CK to try and understand the Red Team’s tactics and counter their attack strategy.

Activity

Name of the Activity

Fastest Finger First

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Fastest Finger First

Role of Red Team
and
Blue Team

Tactics and Techniques -Example

1. The Red Team infects the target with malware using Replication Through Removable Media.

2. The PowerShell to search for privileged accounts.

3. When the Red Team finds a privileged account target, they use an Exploitation for Privilege Escalation.

4. The attacker uses the Remote Desktop Protocol to access other machines on the network.

5. The Red Team collects and infiltrates data back to home base.

MITRE ATT&CK Uses

Plan your strategy

Build your defense

Monitor attack trends

Reference as a guide

Determine threats

Find solution methods

Assess and close gaps

Think-Tank

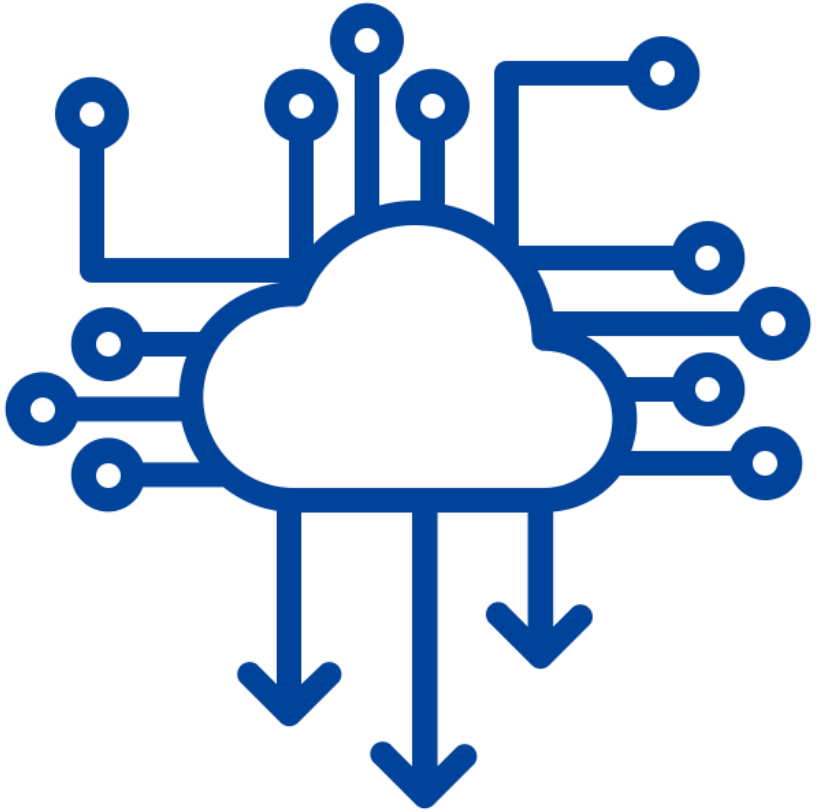
What are the Types of Network?

Created by fae frey
from Noun Project

Types of Networks

There are two different types of networks:

- **Data** network
- **Synchronous** network



Created by Aiden Icons
from Noun Project

Developing a Secure Network

- Access
- Confidentiality
- Authentication
- Integrity
- Non repudiation

Knowledge Check

Name of the Activity

Behind the Door Number

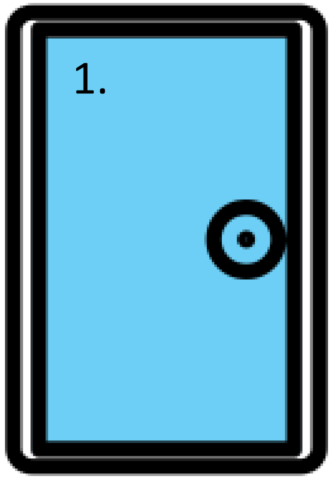
Instructions

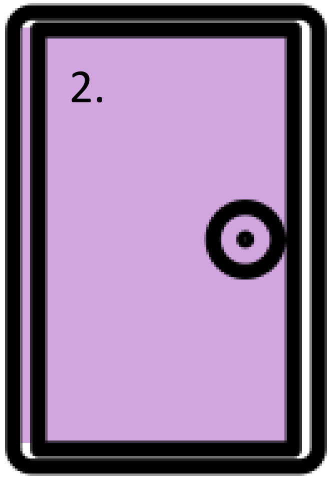
Mode: **In-session**

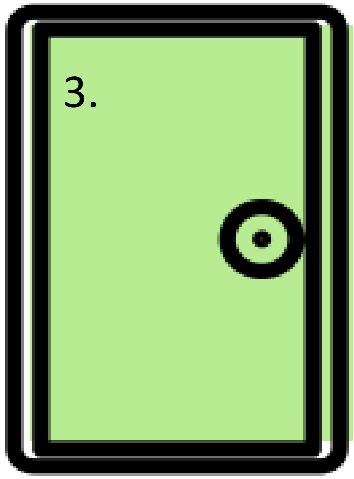
Duration: **5 minutes**

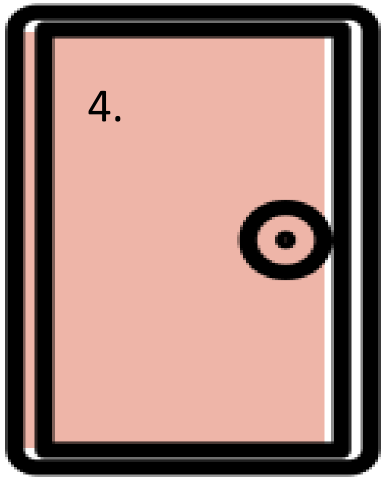
Materials Required: **None**

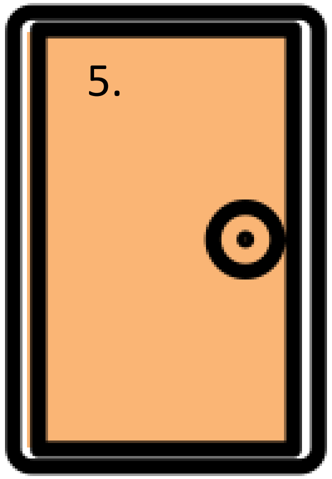
Knowledge Check – Behind the Door Number











Source: Noun project

Summary

In this session, you learnt about:

- Cyber Security Framework
- The Framework Core
- Attack Matrix